10-13-00

GrayCary. TECHNOLOGY'S LEGAL EDGE℠
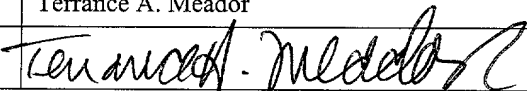
401 B Street, Suite 1700
San Diego, CA 92101-4297
www.graycary.com
O] 619-699-2700
F] 619-699-3452

JC929 U.S. PTO
09/689514
10/12/00

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new non-provisional applications under 37 CFR 1.53(b))

Attorney Docket No.	NDG1140
First Inventor or Application Identifier:	CRAIG ANTHONY FARRELL
Title:	APPARATUS AND METHOD FOR AUTOMATED DISCOVERY AND MONITORING OF RELATIONSHIPS BETWEEN NETWORK ELEMENTS
Express Mail Label No.:	EL185717300US

Application Elements
(See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner For Patents
BOX PATENT APPLICATION
Washington, D.C. 20231

1. __X__ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. __X__ Specification [Total Pages _15_]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R&D
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings *(if filed)*
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. __X__ Drawing(s) (35 USC 113) [Total sheets _3_]

4. __X__ Oath or Declaration [Total Pages _3_]
a. __X__ Newly executed (original or copy)
b. ____ Copy from prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]

i. ____ Deletion of Inventor(s)
Signed statement attached in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ____ Incorporation by Reference *(useable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein

6. ____ Microfiche Computer Program (Appendix)

7. ____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement Verifying identity

ACCOMPANYING APPLICATION PARTS

8 ____ Assignment Papers (cover sheet & document(s))
9. ____ 37 CFR 3.73(b) Statement
(when there is an assignee)
10. ____ English Translation Document (if applicable)
11. ____ Information Disclosure   ____ Copies of IDS
Statement (Form 1449)   Citations
12. ____ Preliminary Amendment
13. _x_ Return Receipt Postcard (CPEP 503)
(Should be specifically itemized)
14. _x_ Small Entity __ Statement filed in prior application,
Statement   Status is still proper and desired
15. ____ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. _x_ OTHER: Express Mail Certification
____ Check # _____ ($ _449.00_)

17. **If a CONTINUING APPLICATION**, check appropriate box and supply the requisite information:
___ Continuation ___ Divisional ___ Continuation-In-Part of prior application no.: ___/_____.
Prior application information: Examiner: _____ Group/Art Unit: _____.

18. CORRESPONDENCE ADDRESS

☐ Customer Number **(25548)**
Or Bar Code Label

OR

25548
PATENT TRADEMARK OFFICE

☐ Correspondence Address Below

NAME	ATTN: Terrance A. Meador **GRAY CARY WARE & FREIDENRICH**
ADDRESS	401 B Street, Suite 1700 San Diego, California 92101 USA

Telephone: 619/699-2652	General Fax No.: 619-236-1048	Patent Group Fax No.: 619/699-3452

Name (print/type)	Terrance A. Meador	Registration No.: (Attorney/Agent)	30,298
Signature	*Terrance A. Meador*	Date	12 October 2000

The USPTO date stamp hereon will acknowledge receipt of:

UTILITY PATENT APPLICATION TRANSMITTAL; FEE
TRANSMITTAL (in duplicate); PATENT APPLICATION (15 PGS); 3
SHEETS OF DRAWINGS; SMALL ENTITY STATEMENT;
DECLARATION; $449.00 FILING FEE CHECK

MAILED 12 OCTOBER 2000 VIA EXPRESS MAIL LABEL NO EL185717300US

APPLICANTS: CRAIG ANTHONY FARRELL ET AL.

FOR: APPARATUS AND METHOD FOR AUTOMATED
DISCOVERY AND MONITORING OF RELATIONSHIPS
BETWEEN NETWORK ELEMENTS

TAM/ Spc / meg

File No.: _____ N061140   103510-165028 _____

EL185717300US

"EXPRESS MAIL" MAILING LABEL NO. _____

DATE OF DEPOSIT: __October 12, 2000_____

**I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED
WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST
OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE
INDICATED ABOVE AND IS ADDRESSED TO THE ASSISTANT
COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231.**

_____**ANTOINETTE LITTLEFIELD**_____
NAME
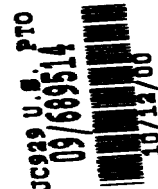
_____
SIGNATURE

GRAYCARY. TECHNOLOGY'S LEGAL EDGE^{SM}

FEE TRANSMITTAL

Attorney Docket No.	NDG1140
First Named Inventor:	CRAIG ANTHONY FARRELL
Application Number	Unknown
Filing Date:	Herewith
Examiner Name:	Unknown
Group/Art Unit:	Unknown

TOTAL AMOUNT OF PAYMENT:	$ 449.00
METHOD OF PAYMENT (check One)	1. __X__ The Commissioner is hereby authorized to charge indicated fees and/or credit any over payment to: Deposit Account No.: 07-1895 Deposit Account Name: GRAY CARY WARE & FREIDENRICH 1. _X_ Charge any Additional Fee Required Under 37 CFR 1.16 and 1.17 2 _X_ Payment Enclosed: _X_ Check _____ Money Order _____ Other
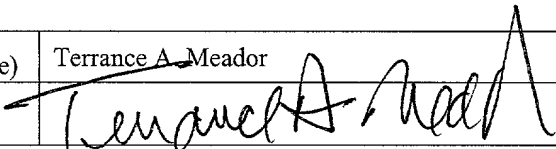
2. UTILITY Basic Filing Fee & Claims

(1) For	(2) No. filed	(3) No. extra	(4) Large Entity	(5) Small Entity	(6) Calculations
Basic Filing Fee	XX	XX	$ 710.00	$355.00	$ 355.00
Total Claims	26 - 20 =	6	X $ 18.00	X $ 9.00	$ 54.00
Independent Claims	4 - 3 =	1	X $ 80.00	X $ 40.00	$ 40.00
Multiple Dependent Claim(s) (if applicable)			$ 270.00	$135.00	$ 000.00
Total of above Calculations =					$ 449.00

Basic Filing Fee	Large Entity	Small Entity	Total
Design filing fee	$ 320.00	$ 160.00	$ 000.00
Reissue filing fee	$ 710.00	$ 355.00	$ 0.00
Provisional filing fee	$ 150.00	$ 75.00	$ 0.00
Total of above Calculations =			$

3. ADDITIONAL FEES

Fee Description	Large Entity	Small Entity	Other
	$	$	$
	$	$	$
	$	$	$
	$	$	$
		TOTAL:	$

Name (print/type)	Terrance A. Meador	Registration No.: (Attorney/Agent)	30,298
Signature		Date	12 October 2000

VERIFIED STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(c)) - SMALL BUSINESS CONCERN

Docket Number (Optional)
NDG1140

Applicant or Patentee: __CRAIG ANTHONY FARRELL, et al.__
Application or Patent No.: _(unknown)_
Filed or Issued: _____(herewith)_____

Title: APPARATUS AND METHOD FOR AUTOMATED DISCOVERY AND MONITORING OF RELATIONSHIPS BETWEEN NETWORK ELEMENTS

I hereby declare that I am
___ the owner of the small business concern identified below:
_x_ an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF SMALL BUSINESS CONCERN __NETWORK HARMONI, INC.__

ADDRESS OF SMALL BUSINESS CONCERN _____12680 High Bluff Drive, Suite 200, San Diego, California 92130_____

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that the rights under the contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention described in:

_X_ the specification filed herewith with title as listed above.
___ the application identified above.
___ the patent identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention must file separate verified statement averring to their status as small entities, and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization having any rights in the invention is listed below:
_x_ No such person, concern or organization exists.
___ Each such person, concern or organization is listed below:

FULL NAME: _____
ADDRESS: _____
    [ ] INDIVIDUAL   [ ] SMALL BUS. CONCERN   [ ] NONPROFIT ORGANIZATION

Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING __JERRY GRAHAM__
TITLE OF PERSON IF OTHER THAN OWNER __Chief Executive Officer__
ADDRESS OF PERSON SIGNING 12680 High Bluff Drive, Suite 200, San Diego, California 92130
SIGNATURE _Jerry Graham_ DATE _10/11/00_

APPARATUS AND METHOD FOR AUTOMATED DISCOVERY AND MONITORING OF RELATIONSHIPS BETWEEN NETWORK ELEMENTS

BACKGROUND OF THE INVENTION

5

1.   Field of the Invention

This invention relates generally to communication networks. In particular, this invention relates to the discovery and monitoring of relationships among network elements within a network.

10

2.   Description of the Related Art

A communication network is made up of interconnected network elements. A network element is any device or computer program that functions as a communication node in the network. Servers are a specific type of network element. The term "server" refers to a computer program that provides services to other computer programs with the same computing platform, or to other computer platforms. A server is also known to refer to a computer platform on which a server program is run. In a client/server networking model, a server is a program that receives and fulfills requests from client programs in the same or other computers. In a specific example, a Web server is the computer program, executed by a computer, that serves requested hypertext markup language (HTML) pages or files.

A client is another specific type of network element. The term "client" refers to a computer program that requests data from a server. For example, a user of a World Wide Web (herein, "Web") browser application makes client requests for hypertext markup language (HTML) pages from Web servers. The browser application is itself a client in a relationship with the Web server that returns the requested HTML file. Thus, the computer program that handles the request and returns the HTML file is the server. Other network elements include the intermediate communication nodes used on a communication route between a server and a client, such as repeaters or routers.

Knowledge of the availability and performance of the network elements is important to the overall operation of the network. Data about network performance is normally gathered by a centralized network management system (NMS). The NMS conventionally operates according to a universal network

5   management protocol for efficient and compatible management across all elements of the network. One such protocol is known as simple network management protocol (SNMP). SNMP governs network management and the monitoring of network devices and their functions.

Network monitoring normally involves the querying of network

10   elements from a centralized vantage point to obtain data about the network elements. The data obtained is usually a listing of network elements, and possibly a listing of application port numbers on which a given network element has a listener process. The data generally provides an atomistic view of network elements, by identifying clients, servers, and other network elements of the network, without defining any

15   further relationship between any given network element and the rest of the network.

Two main methods presently exist for discovering network clients, servers, other network elements, and their applications. One method is known as "ping flooding." In ping flooding, or its variants, a packet source floods the network with packets. The packet source may be a central server, the NMS, or a distributed

20   agent within the network. The packet source then monitors the network to see which network elements respond to a packet. Accordingly, any network elements that respond are "discovered" by the ping flooding process.

A second method is known as "port sweeping," a finer-grained network discovery and monitoring method that extends on ping flooding. In port

25   sweeping, once a network element has been discovered, an attempt is made, usually by the packet source, to connect to the network element using a number of connection ports on the network element platform. As different applications "listen" to the network on different ports, port sweeping will reveal what applications on the network element, also known as "services," are currently available or "listening."

An additional method of network discovery includes a monitoring process, and is used for discovering which applications are used or available on a host network element. Such a method includes having the host provide information on its hosted and available applications. An example of this method is a host resources management information base (MIB), a description of a set of network objects that can be managed using SNMP, which is described in MIB RFC 1514, for example.

Port sweeping, ping flooding, and other current network discovery and monitoring methods are limited to providing data only about the existence of network elements, and do not extend to defining relationships between the network elements. Furthermore, existing network management methods do not extend to discovering and monitoring application-layer relationships.

The problems and limitations of prior art monitoring methods are evident in a specific example in which such methods are used. A traffic generator is a network apparatus used to generate, or simulate, traffic conditions for purposes of data collection and benchmarking. Current traffic generators work by "recording" a transaction which will be repeated many times from various vantage points. The transaction could be a simulated application process that is provided by a server to a client. Once recorded, the transaction is then provided to various remote agents within the network for execution, and metrics, such as response time, are calculated for simulated users at those remote locations. The traffic generators in this example simply replay the traffic from multiple locations to the same application server. The problem is that different remote locations may use different servers to provide the same applications.

SUMMARY OF THE INVENTION

This invention relates to a distributed agent configured for discovering elements of a network and monitoring relationships between the network elements. Preferably, the network elements include, without limitation, clients, servers, intermediate communication nodes and applications programs. According to the invention, an agent is hosted on at least one network element. The agent discovers

what applications are running on the host network element, and which servers are used for serving each of the discovered applications. The discovery is preferably, although not necessarily from the point of view of a client of the discovered applications and application servers. The invention also discovers relationships

5 among clients or other network elements in the network. The agent may also reside on the server to discover which clients use it for which applications.

Another embodiment of the invention includes the steps of hosting an agent on at least one of a plurality of interconnected network elements, where the agent is configured to gather application data representing a network-based

10 application for use by the host network element. Using the agent, application traffic is monitored between the application and at least one other network element.

Another embodiment of the invention includes the steps of hosting an agent on at least one of a plurality of interconnected network elements, and gathering application data with the agent. The application data represents a network-based

15 application for use by the host network element. A further step is monitoring, using the agent, application traffic between the application and any other network element having a relationship with the application.

In still yet another embodiment of the invention, a method includes the steps of hosting an agent on at least one of a plurality of interconnected network

20 elements, for autonomously gathering application data with said hosted agent, and using said agent, monitoring application traffic between the application and any other network element having a relationship to the application.

In yet another embodiment of the invention, an apparatus for monitoring a network includes an agent being configured to gather application data

25 representing a network-based application, and further being configured to monitor application traffic between the application and any network element in the network having a relationship to the application. The apparatus further includes an agent hosting means for hosting the agent on one of a plurality of interconnected network elements.

30

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1 is a diagram of a network topology in which the present invention is used.

FIG. 2 is a flow chart illustrating a method of monitoring a network according to an embodiment of the present invention.

FIG. 3 is a functional diagram of an agent apparatus and monitoring system according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. 1 shows a simplified network topology as an example of a communication network for which the present invention is suited. A network 100 includes a plurality of interconnected network elements. The network elements include servers 110 connected with clients 120 via one or more intermediate network elements 130. It should be understood that the network illustrated in FIG. 1 is described herein for purposes of illustrating exemplary embodiments of the present invention. Those skilled in the art would recognize that the present invention may be used in more complex networks, or that servers and clients may be directly connected, i.e. sharing the same computer device, or that the number and extent of intermediate network elements may vary between communicating network elements. Those skilled in the art will also recognize that computers may also be both clients and servers either separately or concurrently. For example, a web server machine serving HTML pages may also run a web browser and hence be a client as well.

In accordance with an embodiment of the present invention, each clients 120 and the servers 110 represents one or more applications employed in a certain manner by the respective network elements. The servers 110 receive and respond to requests from the clients 120. One example of an application in the client/server model is electronic mail ("e-mail"), where a client 120 includes an e-mail program that sends and receives e-mail files via an e-mail server 110. Another example application is Internet service. A client 120 runs an Web browsing

application program for searching the Web, and requests from the client 120 are received and fulfilled by a Web server 110 running a Web-serving application.

In an embodiment of the invention, a distributed agent is a program running on at least one of the network elements, such as one of the servers 110 or
5   clients 120, to monitor application traffic in order to discover a relationship between clients, servers, applications, and the intermediate network elements. By employing a plurality of distributed agents in the network, a complete application-level topology and relationship structure may be ascertained. According to the embodiment, a relationship may be defined in many ways, such as which clients use which servers,
10 for which applications, and what intermediate network elements are used to establish the application-level connection between clients and servers.

Referring now to FIG. 2, a method 200 of monitoring a network begins at start block 205, in which network elements of a network are configured with distributed network-monitoring agents. In a specific preferred embodiment of the
15 invention, all of the client network elements include an agent. However, in alternative embodiments, any single or combination of network elements, including servers, may contain an agent. The agent may be pre-installed at the network element, or downloaded according to any of the known file transfer protocols currently in use with networked communications.

20 At function block 210, a standard host discovery process is executed. The discovery process may be any known process, such as ping flooding and/or port sweeping described above. Host discovery is executed at function block 210 to discover which network elements are running the application-monitoring agent. Any network element hosting an agent or running an agent program is referred to herein as
25 a host network element. In other words a network element that is discovered is referred to as an "instrumented" node of the network at block 215. All instrumented nodes are thus self-identified and discoverable by a central NMS.

At function block 220, each host network element's agent discovers which applications are installed on their host. Function block 220 is preferably
30 executed in accordance with the Host Resources RFC 1514 or equivalent

management information base (MIB) functionality, according to an exemplary embodiment of the invention. Such functionality requires the agent to support certain selected MIB specifications.

5   After the applications installed on the host are obtained, the agent begins monitoring application traffic for each application. From the vantage point of the host network element, gathering application traffic data by monitoring application traffic enables discovery by the agent of a client/server relationship of each application, at function block 230. Thus, illustrated with reference to block 230, the agent determines which clients are communicating with which servers for running

10   certain networking applications, and the determination is made at the application level.

When the servers of each application are known, i.e. the client/server relationship is established for each application. At function block 235 the agent executes a route tracing process to trace the route of the application traffic between

15   the server and the client. With reference to FIG. 1, one or more intermediate network elements may be deployed between each server and its respective client or clients. Further, each client may access more than one server for running more than one application, or for running the same application. The intermediate network elements define successive nodes in a route between a server 110 and a client 120 for each

20   discovered relationship as described above. Having thus determined the route and the intermediate network elements used, the agent obtains a complete topological view of the network, from the application-level perspective.

Auto discovery of applications, servers, and intermediate network elements by client-hosted distributed agents, in accordance with the present invention,

25   provides a unique "client view" of the network and networked applications. The client view, in turn, provides valuable information about the interrelationships of network elements that is otherwise very difficult and time consuming to obtain.

FIG. 3 shows a system 300 for monitoring a network including an agent apparatus 317. In a preferred exemplary embodiment, the agent 317 is hosted

30   on a client 315 makes up a portion of a first network element platform 310. A second

network element platform 320 includes a server 325, and has a database 327. The database 327 stores a network management system, configured to monitor the status of the network to which the network element platforms 310 and 320 belong, in accordance with standard practice of network management operation.

5   The agent 317 is configured to communicate with the database 327 via a connection that supports SNMP. In accordance with the present invention, the agent 317 monitors network operations from the point of view of the client 315, including any applications running on the client, and interrelationships with the rest of the network. Data monitored and collected by the agent 317 is provided in an

10   electronic document formatted according to a MIB specification, which is then reported to the database via the SNMP connection. The network management system uses the data provided by the agent for more detailed and useful monitoring of the network, according to the teachings of the present invention.

Referring back to FIGS. 1 and 2, example uses of the agent apparatus

15   of the present invention will now be described. If an agent is deployed on all clients 120 (C1 – C5), or on all the servers 110 (S1 – S2), execution of the method 200 might yield, for example, the following information:

C1 uses S1 for e-mail;

C1 uses S1 for web serving;

20   C2 uses S2 for e-mail;

C2 uses S2 for web serving;

C3 uses S1 for e-mail;

C3 uses S1 for web serving;

C4 uses S2 for e-mail;

25   C4 uses S2 for web serving;

C5 uses S1 for e-mail;

C5 uses S2 for web serving;

Event Correlation

The client, server, and application information obtained by execution

30   of a method according to the present invention is provided to an event correlator. An

C4 uses S2 for e-mail;

C4 uses S2 for web serving;

C5 uses S1 for e-mail;

C5 uses S2 for web serving;

5 <u>Event Correlation</u>

The client, server, and application information obtained by execution of a method according to the present invention is provided to an event correlator. An event correlator is an apparatus, such as a processor or a computer program, which correlates operations with corresponding network elements. The event correlator

10 would generate statistics such as, for example, if S1's e-mail serving application fails, application traffic "events" would still be obtained from C1, C2, C3 and C5, but not from C4. C5 would report failure of its e-mail server but not failure of its web server. Thus, the event correlator, using data accumulated according to the invention, extends conventional network diagnostic systems that may determine "the server is up/down"

15 to now enable a determination such as "the web serving application still works on S1 but e-mail is down" for example. The monitoring data provided by the present is therefore useful for fine-grained application layer diagnostics.

<u>Root Cause Analysis</u>

Network analysis tools can utilize data provided by the agent apparatus

20 according to the present invention to diagnose a root cause of an event, such as a failure or interrupt. The present invention extends conventional failure diagnostics to incorporate information about the application layer of a network for more effective isolation of failure points in the network.

<u>Capacity Planning and Risk Analysis</u>

25 In addition to providing a physical and logical topological view of a network, the present invention also provides an application-specific view of the network. For example, for a server that runs a particular application which it serves to a number of clients, the present invention can provide a view of the network from that application's view on the server. In risk analysis, knowing which application or

network services will be affected by a failure of a specific network element can be provided by the present invention and assessed to minimize risk. For capacity planning and load balancing, knowing which servers and clients rely on each other for services and applications allows for more efficient planning of resources, such as

5   which resources to upgrade, etc.

Software Licensing

The present invention provides data about which servers of a particular application and/or service provides necessary information for auditing of software licenses in a distributed networked environment. For example, if a product is

10   installed on a server is a C++ compiler, the present invention assists tracking those clients that do not host the compiler, but nevertheless use it.

Traffic Generator

Traffic generators repeatedly transmit pre-programmed data over a network to remote agents in order to measure response time, etc. The present

15   invention can be used to supplement the functions provided by traffic generators by providing information about which server is accessed and used from a specific client location. Simulated communication playback could be reconfigured and/or automatically modified to continually retransmit the pre-programmed data using the appropriate application server for a particular client.

20   These and other uses, embodiments, combinations and modifications of the present invention will occur readily to those of ordinary skill in the art in view of these teachings. Therefore, this invention is to be limited only by the following claims, which include all such embodiments and modifications when viewed in conjunction with the above specification and accompanying drawings.

25

WE CLAIM:

CLAIMS

1.   A method of monitoring a network, comprising:

hosting an agent on at least one of a plurality of interconnected network elements, wherein the agent is configured to gather application data

5   representing a network-based application for use by the host network element; and

using the agent, monitoring application traffic between the application and at least one other network element.

2.   The method according to claim 1, further comprising tracing a

10   route of the application traffic with the agent.

3.   The method according to claim 2, wherein the tracing the route includes identifying a server of the application.

15   4.   The method according to claim 3, wherein the tracing the route includes identifying a client of the server.

5.   The method according to claim 4, wherein the tracing the route includes identifying any intermediate network elements along the route between the

20   server and the client.

6.   The method according to claim 4, wherein the client is the host network element.

25   7.   The method according to claim 1, wherein the agent is further configured to identify a relationship between the application and the other network element based on the application traffic.

8.   The method according to claim 7, wherein the relationship is a

30   client/server relationship.

9.   The method according to claim 7, wherein the relationship is a peer-to-peer relationship.

5   10.   A method of monitoring a network, comprising:

hosting an agent on at least one of a plurality of interconnected network elements;

gathering, with said agent, application data representing a network-based application for use by the host network element; and

10   using said agent, monitoring application traffic between the application and any other network element having a relationship with the application.

11.   The method according to claim 10, wherein the monitoring further comprises tracing a route of said application traffic.

15   12.   The method according to claim 10, wherein the application data includes data representing a server of the application.

13.   The method according to claim 10, further comprising

20   reporting the application data and application traffic data to a network management system.

14.   The method according to claim 13, wherein the network management system is hosted on a different one of the network elements.

25   15.   The method according to claim 12, wherein the monitoring further comprises identifying any intermediate network elements between the server and a client traversed by said application traffic.

16.   The method according to claim 15, wherein the monitoring further comprises tracing a route between the server and the client.

17.   The method according to claim 16, wherein the route forms an topology of network elements for the application.

18.   The method according to claim 10, further comprising repeating the gathering application data and the monitoring application traffic for each network-based application used by the host network element.

19.   The method according to claim 18, wherein the monitoring further comprises tracing a route between a server and a client of each application.

20.   The method according to claim 19, wherein the route for each application includes any intermediate network elements traversed by the application, to form a network topology of all of the monitored applications.

21.   A method of monitoring a network, comprising:

hosting an agent on at least one of a plurality of interconnected network elements, for autonomously gathering application data with said hosted agent, wherein the application data represents a network-based application for use by the host network element; and

using said agent, monitoring application traffic between the application and any other network element having a relationship to the application.

22.   An apparatus for monitoring a network, comprising:

an agent being configured to gather application data representing a network-based application, and further being configured to monitor application traffic between the application and any network element in the network having a relationship to the application; and

agent hosting means for hosting the agent on one of a plurality of interconnected network elements.

23.   The apparatus according to claim 22, wherein the agent is

5   further configured to discover a server of the application, and to trace a route of the application traffic from the server through any intermediate network elements to the client.

24.   The apparatus according to claim 23, wherein the client

10   includes the agent hosting means.

25.   The apparatus according to claim 22, wherein the agent is further configured to communicate a report externally from the agent hosting means.

15   26.   The apparatus according to claim 25, wherein the agent hosting means includes a memory within the hosting network element.

APPARATUS AND METHOD FOR AUTOMATED DISCOVERY AND MONITORING OF RELATIONSHIPS BETWEEN NETWORK ELEMENTS

ABSTRACT OF THE INVENTION

5

      A network discovery and monitoring apparatus and method of using the same. An apparatus includes an agent configured for being hosted on one of a plurality of interconnected network elements that form at least a portion of a communication network. A method includes the agent gathering application data representing a

10   network-based application that is accessible from the network element hosting the agent. The agent monitors application traffic between each discovered application and any network element having a relationship to the application. A result of the monitoring is a relational topology, at the application layer, of the network elements in the network.

15

FIG. 1

```
                    ┌─────────────┐
                    │    START    │ ⟵ 205
                    └─────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │    STANDARD HOST         │ ⟵ 210
              │    DISCOVERY             │
              └──────────────────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │  DISCOVER INSTRUMENTED   │ ⟵ 215
              │       NODES              │
              └──────────────────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │ DISCOVER APPLICATIONS ON │ ⟵ 220
              │ EACH INSTRUMENTED NODE   │
              └──────────────────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │   MONITOR APPLICATION    │ ⟵ 225
              │   TRAFFIC FROM           │
              │   INSTRUMENTED NODE      │
              └──────────────────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │ DETERMINE CLIENT/SERVER  │ ⟵ 230
              │   RELATIONSHIP           │
              └──────────────────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │  TRACE ROUTE OF PACKETS  │ ⟵ 235
              │  IN CLIENT/SERVER        │
              │  RELATIONSHIP            │
              └──────────────────────────┘
                           │
                           ▼
              ┌──────────────────────────┐
              │ DETERMINE INTERMEDIATE   │ ⟵ 240
              │ NETWORK ELEMENTS         │
              └──────────────────────────┘
                           │
                           ▼
                    ┌─────────────┐
                    │     END     │ ⟵ 245
                    └─────────────┘
```

200

FIG. 2

CLIENT 310

315

AGENT 317

DATA

MIB

SERVER 320

325

DATABASE 327

SNMP 330

300

FIG. 3

DECLARATION FOR PATENT APPLICATION

_X_ Declaration Submitted With Initial Filing   **OR**   ___ Declaration Submitted After Initial Filing

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship is as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

APPARATUS AND METHOD FOR AUTOMATED DISCOVERY AND MONITORING OF RELATIONSHIPS BETWEEN NETWORK ELEMENTS

the specification of which
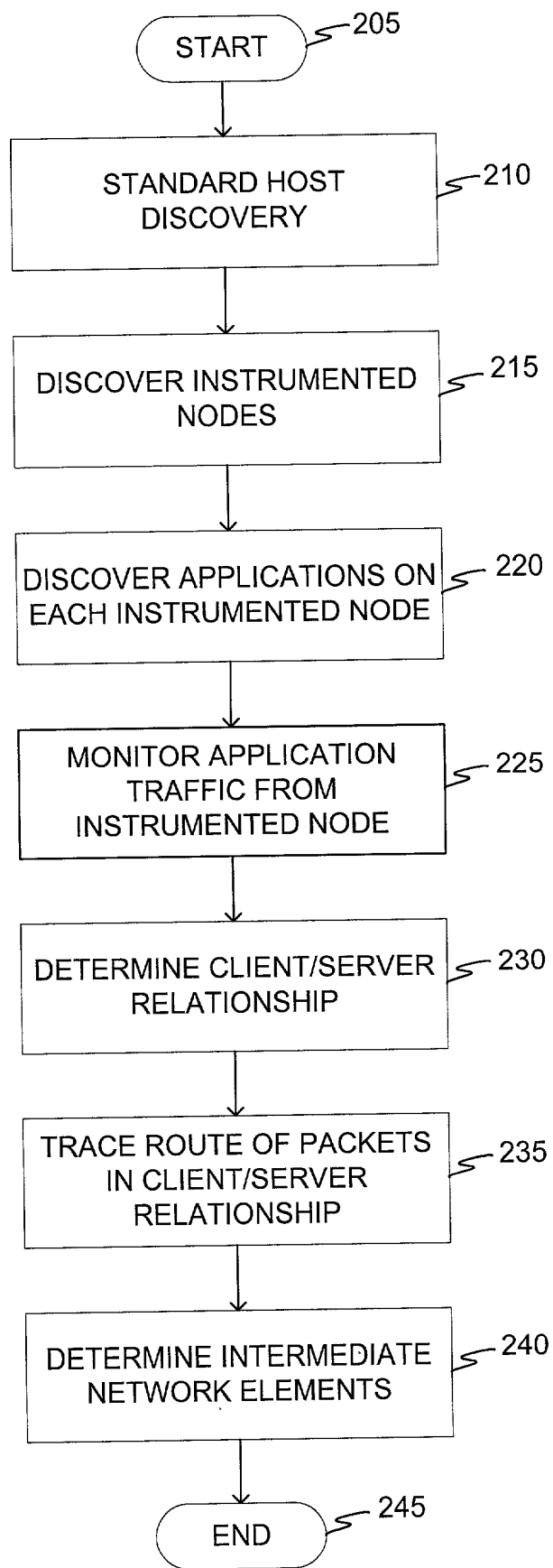
_X_ is attached hereto.

___ was filed on _____, 2000 as U.S. Application Serial No. _____

_____ and was amended on _____ if applicable (the "Application").

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability of the subject matter of the Application as defined in Title 37, Code of Federal Regulations ("C.F.R."), § 1.56.

I hereby claim foreign priority benefits under Title 35 United States Code § 119 (a)-(d) or § 365(b) of any foreign applications for patent or inventors certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America listed below and have been identified below by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Numbers	Country	Foreign Filing Date (MM/DD/YYY)	Priority Not Claimed	Certified Copy Attached	
				YES	NO

With respect to the Application, I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

Application Number(s)	Filing Date (MM/DD/YYYY)

With respect to the Application, I hereby claim the benefit under 35 U.S.C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of the application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability of the subject matter of the Application as defined in Title 37, C.F.R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of the Application:

U.S. Parent Application Number	PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer Number	25548

25548

PATENT .TRADEMARK OFFICE

**Place Customer Number
Bar Code Label Above**

Please direct all correspondence to:

Terrance A. Meador
Gray Cary Ware & Freidenrich
401 B Street, Suite 1700
San Diego, CA 92101-4297

Phone: 619/699-2652 - Fax: 619/699-3452

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole Or First Inventor (*First, Middle, Family Name or Surname*)	CRAIG ANTHONY FARRELL	
Inventor Signature	*[signature]*	Date: 10/11/00
Residence Address	3950 Tynebourne Circle, San Diego, California 92130	
Post Office Address	3950 Tynebourne Circle, San Diego, California 92130	
Citizenship	Australia	

Full Name of Second Inventor (*First, Middle, Family Name or Surname*)	THANES DUKE TANTIPRASUT	
Inventor Signature	*[signature]*	Date: 10/11/00
Residence Address	12570 Carmel Creek Road, Apt. 80, San Diego, California 92130	
Post Office Address	12570 Carmel Creek Road, Apt. 80, San Diego, California 92130	
Citizenship	Australia	

Full Name of Third Inventor (*First, Middle, Family Name or Surname*)		
Inventor Signature		
Residence Address		
Post Office Address		
Citizenship		